Appeal Brief
I hereby certify that this paper (along with any paper referred to as being attached or enclosed) is being transmitted via the Office electronic filing system in accordance with § 1.6(a)(4).

Dated: March 7, 2011
Electronic Signature for Isaac T. Slutsky: /Isaac T. Slutsky/

Docket No.: 00-4045
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Russell A. Fink et al.

Application No.: 09/928,133 | Confirmation No.: 6468

Filed: August 10, 2001 | Art Unit: 2437

For: METHOD AND APPARATUS FOR PROVIDING ADAPTIVE SELF-SYNCHRONIZED DYNAMIC ADDRESS TRANSLATION AS AN INTRUSION DETECTION SENSOR | Examiner: T. Teslovich

APPEAL BRIEF

MS Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

This Appeal Brief is filed pursuant to 37 C.F.R. § 41.37 in furtherance of the Notice of Appeal filed on January 7, 2011. This Appeal Brief appeals the decision of the Examiner in the Final Office Action dated October 8, 2010 ("Final Office Action") and the Advisory Action dated January 5, 2011 ("Advisory Action"). This application was filed on August 10, 2001.

The fees required under § 41.20(b)(2) are dealt with in the accompanying TRANSMITTAL OF APPEAL BRIEF.

TABLE OF CONTENTS

This brief contains items under the following headings as required by 37 C.F.R. § 41.37 and M.P.E.P. § 1205.02:

TABLE OF CONTENTS

I. REAL PARTY IN INTEREST

The real party in interest of the present application, solely for purposes of identifying and avoiding potential conflicts of interest by board members due to working in matters in which the member has a financial interest, is Verizon Communications Inc. and its subsidiary companies, which currently include Verizon Business Global, LLC (formerly MCI, LLC) and Cellco Partnership (doing business as Verizon Wireless, and which includes as a minority partner affiliates of Vodafone Group Plc). Verizon Communications Inc. or one of its subsidiary companies is an assignee of record of the present application.

II. RELATED APPEALS AND INTERFERENCES

Applicants (hereinafter "Appellants") are not aware of any related appeals or interferences that would affect the Board's decision on the current appeal.

III. STATUS OF CLAIMS

Claims 21-24 were previously canceled. Claims 1-20 and 25-32 are pending, stand rejected, and are the subject of this appeal. Claims 1, 6, 11 and 16 are written in independent form. Each of the appealed claims is reproduced in Appendix A to this Appeal Brief.

IV. <u>STATUS OF AMENDMENTS</u>

Appellants did not submit, and the Examiner did not enter, any amendments to the application subsequent to the Final Office Action dated October 8, 2010. Accordingly, the claims as presented in the Response dated December 7, 2010 are the subject of this appeal and are reproduced in Appendix A to this paper.

V. SUMMARY OF CLAIMED SUBJECT MATTER

The following is a concise explanation of the subject matter defined in at least each of the independent claims involved in the appeal, as required by 37 C.F.R. § 41.37(c)(1)(v). The following explanation is not intended to be used to construe the claims, which are believed to speak for themselves. Nor do Appellants intend the following explanation to modify or add any claim elements, or to constitute a disclaimer of any equivalents to which the claim would otherwise be entitled. Nor is any reference to certain preferred embodiments herein intended to disclaim other possible embodiments.

This summary of the presently claimed subject matter indicates certain portions of the specification (including the drawings) that provide examples of embodiments of elements of the claimed subject matter. It is to be understood that other portions of the specification not cited herein may also provide examples of embodiments of elements of the claimed subject matter. It is also to be understood that the indicated examples are merely examples, and the scope of the claimed subject matter includes alternative embodiments and equivalents thereof. References herein to the specification are thus intended to be exemplary and not limiting.

A. Claim 1

Claim 1 recites an apparatus for detecting adversarial activity on a network (e.g., Specification, page 9, lines 5-20), comprising:

a memory configured to store a host table (e.g., Specification, page 9, lines 10-11);

a key exchanger configured to repeatedly derive a cipher key (e.g., Specification, page 9, lines 11-12) such that the resulting cipher key changes over time (e.g., Specification, page 18, line 21 – page 19, line 12);

a translator configured to restore predetermined portions of packet header information of a data packet (e.g., Figure 3; Figure 8, step Figure 9, step S902; Specification, page 22, line 16 – page 23, line 2; page 20, Table 1, page 22, Table 2), the packet header information including a network portion of a destination address routable over a wide area network and an encrypted host portion of the address identifying a destination host (e.g., Specification, page 17, line 16 – page 18, line 6; page 20, Table 1, page 22, Table 2), the restoration including to:

extract, from the packet header information, predetermined portions of packet header data including the encrypted host portion of the address (e.g., Specification, page 23, lines 2-8),

decrypt, according to a cipher algorithm keyed by the cipher key, the extracted packet header data to determine a restored address (e.g., Specification, page 23 lines 8-10; page 53, lines 5-15), and

place the restored address back into the packet header information of the data packet (e.g., Specification, page 23, lines 10-15);

a mapping device configured to map the restored address to the host table (e.g., Figure 9, step S903A; Specification, page 9, lines 16-18; page 52, lines 10-11);

a host resolution device configured to issue a request to the network to resolve the restored address when the restored address does not match an entry in the host table (e.g., Figure 9, steps S903B and S905A; Specification, page 52, line 12 – page 53, line 3; page 53, lines 10-22) and to supplement the host table with the restored address upon receipt of a reply to the request that indicates that the restored address is valid (e.g., Figure 9, step S905B and S906; Specification, page 52, line 12 – page 53, line 3; page 53, lines 17-22); and

an actuator configured to trigger a security device when the restored address does not match an entry in the host table (e.g., Figure 9, step S908; Specification, page 9, lines 16-18; page 54, lines 1-8).

B. Claim 6

Claim 6 recites a method for detecting adversarial activity on a network (e.g., Specification, page 10, lines 1-10), comprising:

storing a host table (e.g., Specification, page 10, line 3);

repeatedly deriving a cipher key (e.g., Specification, page 10, lines 3-6) such that the resulting cipher key changes over time (e.g., Specification, page 18, line 21 – page 19, line 12);

restoring predetermined portions of packet header information of a data packet (e.g., Figure 3; Figure 8, step Figure 9, step S902; Specification, page 22, line 16 – page 23, line 2; page 20, Table 1, page 22, Table 2), the packet header information including a network portion of a destination address routable over a wide area network and an encrypted host portion of the address

identifying a destination host (e.g., Specification, page 17, line 16 – page 18, line 6; page 20, Table 1, page 22, Table 2), the restoring including:

extracting, from the packet header information, predetermined portions of packet header data including the encrypted host portion of the address (e.g., Specification, page 23, lines 2-8),

decrypting, according to a cipher algorithm keyed by the cipher key, the extracted packet header data to determine a restored address (e.g., Specification, page 23 lines 8-10; page 53, lines 5-15) and

placing the restored address back into the packet header information of the data packet (e.g., Specification, page 23, lines 10-15);

mapping the restored address to the host table (e.g., Figure 9, step S903A; Specification, page 9, lines 16-18; page 52, lines 10-11);

issuing a request to the network to resolve the restored address when the restored address does not match an entry in the host table (e.g., Figure 9, steps S903B and S905A; Specification, page 52, line 12 – page 53, line 3; page 53, lines 10-22) and supplementing the host table with the restored address upon receipt of a reply to the request that indicates that the restored address is valid (e.g., Figure 9, step S905B and S906; Specification, page 52, line 12 – page 53, line 3; page 53, lines 17-22); and

triggering a security device when the restored address does not match an entry in the host table (e.g., Figure 9, step S908; Specification, page 9, lines 16-18; page 54, lines 1-8).

C. Claim 11

Claim 11 recites a device for detecting adversarial activity on a network (e.g., Specification, page 10, lines 12-22), comprising:

means for storing a host table (e.g., Specification, page 10, lines 12-14);

means for repeatedly deriving a cipher key (e.g., Specification, page 10, lines 14-15) such that the resulting cipher key changes over time (e.g., Specification, page 18, line 21 – page 19, line 12);

means for restoring predetermined portions of packet header information of a data packet (e.g., Figure 3; Figure 8, step Figure 9, step S902; Specification, page 22, line 16 – page 23,

line 2; page 20, Table 1, page 22, Table 2), the packet header information including a network portion of a destination address routable over a wide area network and an encrypted host portion of the address identifying a destination host (e.g., Specification, page 17, line 16 – page 18, line 6; page 20, Table 1, page 22, Table 2), the means for restoring including:

means for extracting, from the packet header information, predetermined portions of packet header data including the encrypted destination host portion of the address (e.g., Specification, page 23, lines 2-8),

means for decrypting, according to a cipher algorithm keyed by the cipher key, the extracted packet header data to determine a restored address (e.g., Specification, page 23 lines 8-10; page 53, lines 5-15) and

means for placing the restored address back into the packet header information of the data packet (e.g., Specification, page 23, lines 10-15);

means for mapping the restored address to the host table (e.g., Figure 9, step S903A; Specification, page 9, lines 16-18; page 52, lines 10-11);

means for issuing a request to the network to resolve the restored address when the restored address does not match an entry in the host table (e.g., Figure 9, steps S903B and S905A; Specification, page 52, line 12 – page 53, line 3; page 53, lines 10-22) and supplementing the host table with the restored address upon receipt of a reply to the request that indicates that the restored address is valid (e.g., Figure 9, step S905B and S906; Specification, page 52, line 12 – page 53, line 3; page 53, lines 17-22); and

means for triggering a security device when the restored address does not match an entry in the host table (e.g., Figure 9, step S908; Specification, page 9, lines 16-18; page 54, lines 1-8).

D. Claim 16

Claim 16 recites a bastion host comprising at least one computing device adapted for processing packet header information of a data packet (e.g., Specification, page 11, lines 1-11), the bastion host being configured to:

store a host table (e.g., Specification, page 11, line 4);

repeatedly derive a cipher key (e.g., Specification, page 11, line 4) such that the resulting cipher key changes over time (e.g., Specification, page 18, line 21 – page 19, line 12);

restore predetermined portions of packet header information of a data packet (e.g., Figure 3; Figure 8, step Figure 9, step S902; Specification, page 22, line 16 – page 23, line 2; page 20, Table 1, page 22, Table 2), the packet header information including a network portion of a destination address routable over a wide area network and an encrypted host portion of the address identifying a destination host (e.g., Specification, page 17, line 16 – page 18, line 6; page 20, Table 1, page 22, Table 2), the restoring including to:

extract, from the packet header information, predetermined portions of packet header data including the encrypted host portion of the address (e.g., Specification, page 23, lines 2-8),

decrypt, according to a cipher algorithm keyed by the cipher key, the extracted packet header data to determine a restored address (e.g., Specification, page 23 lines 8-10; page 53, lines 5-15) and

place the restored address back into the packet header information of the data packet (e.g., Specification, page 23, lines 10-15);

map the restored address to the host table (e.g., Figure 9, step S903A; Specification, page 9, lines 16-18; page 52, lines 10-11);

issuing a request to the network to resolve the restored address when the restored address does not match an entry in the host table (e.g., Figure 9, steps S903B and S905A; Specification, page 52, line 12 – page 53, line 3; page 53, lines 10-22) and supplement the host table with the restored address upon receipt of a reply to the request that indicates that the restored address is valid (e.g., Figure 9, step S905B and S906; Specification, page 52, line 12 – page 53, line 3; page 53, lines 17-22); and

trigger a security device when the restored address does not match an entry in the host table (e.g., Figure 9, step S908; Specification, page 9, lines 16-18; page 54, lines 1-8).

E. Claim 29

Claim 29 recites a device as set forth in Claim 11, the host portion of the address having been translated without the network portion also being translated (e.g., Specification, page 20, line

17 – page 21, line 9; page 22, lines 4-14 and Table 2), and wherein said means for translating predetermined portions of packet header information is configured to restore the host portion of the address without also restore the network portion of the address (e.g., Specification, page 22, line 17 – page 23, line 15).

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

The Final Office Action set forth the following ground for rejecting Appellants' claims to be reviewed in this appeal:

1. Claims 1-20 and 25-32 were rejected under 35 U.S.C. 102(e) as allegedly being anticipated by U.S. Pat. Pub. No. 2002/0184390 to Hasan Alkhatib ("Alkhatib").

VII. ARGUMENT

A. Ground Of Rejection No. 1: Claims 1-20 and 25-32 Are Patentable Over Alkhatib

MPEP § 2131 states that to anticipate a claim, the reference must teach every element of the claim. "A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). "'The identical invention must be shown in as complete detail as is contained in the . . . claim.' See *Richardson v. Suzuki Motor Co.*, 868 F. 2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989)." As detailed in the subsections below, each and every element as set forth in the claims is not found in Alkhatib. Therefore, for at least the following reasons, the Section 102(e) rejection of claims 1-20 and 25-32 should be reversed and the claims allowed.

1. Independent Claim 1

Independent claim 1 was rejected under Section 102(e) as allegedly being anticipated by Alkhatib. However, Alkhatib fails to anticipate at least (a) "a key exchanger configured to repeatedly derive a cipher key such that the resulting cipher key changes over time;" (b) to "decrypt, according to a cipher algorithm keyed by the cipher key, the extracted packet header data;" (c) to "decrypt . . . to determine a restored address;" and (d) to "place the restored address back into the packet header information of the data packet," each as recited in the context of claim 1. Thus, for at least the reasons discussed in subsections (a)-(d) below, independent claim 1 and all claims that depend therefrom are patentable over Alkhatib.

a. *"a key exchanger configured to repeatedly derive a cipher key such that the resulting cipher key changes over time"*

Independent claim 1 recites in part "a key exchanger configured to repeatedly derive a cipher key such that the resulting cipher key changes over time." In the Final Office Action, paragraph 67 of Alkhatib was cited as allegedly disclosing these recitations. (Final Office Action, page 4.) In response to previous arguments, the Examiner further stated that "Alkhatib provides for the encoding/translation of addresses in order to provide more efficient use of storage space, security and compatibility (par 36)." (Office Action, page 2.) Alkhatib mentions "unencrypting,"

but fails to anticipate "a key exchanger configured to repeatedly derive a cipher key" as recited by claim 1, let alone "a key exchanger configured to repeatedly derive a cipher key such that the resulting cipher key changes over time," as further recited by claim 1.

More specifically, Alkhatib discloses a "data unit" addressed to a global address of a "domain name router," where the "data unit" additionally includes a "domain name." (e.g., Alkhatib, Abstract.) Alkhatib further discloses that "the Domain Name Router [(DNR)] receives the data, extracts the destination's domain name from the data, translates that domain name to a local address in its stub network and sends the data to the destination." (Alkhatib, paragraphs 12 and 14.) In Alkhatib, "the source and destination's domain names are added to Options field 22" and "the two domain names can be encoded, compressed, encrypted or otherwise altered to provide more efficient use of storage space, security or compatibility." (Alkhatib, paragraph 36.) Paragraph 36 of Alkhatib further discloses that:

> In embodiments where the domain name is encoded, encrypted, compressed, etc., the information stored is said to represent the domain name. That is, an entity can read that information and extract (or identify) the domain name from that information. That extraction or identification can be by unencoding, decoding, decompressing, unencrypting, etc.

(Id.) Cited paragraph 67 describes a portion of Alkhatib Figure 10, and in particular discloses the steps "receive packet," "identify domain name," "translate," and "send data." As cited by the Examiner, "if the domain names are compressed, encrypted, encoded, etc., then DNR 148 would need to decode, decompress, unencrypt, etc." (Alkhatib, paragraph 67.)

However, Alkhatib fails to disclose or suggest any details of these decode, decompress or unencrypt operations. Lacking disclosure of any of these details, Alkhatib at least fails to anticipate "a key exchanger configured to repeatedly derive a cipher key," let alone "a key exchanger configured to repeatedly derive a cipher key such that the resulting cipher key changes over time," each as recited in the context of claim 1.

In the Final Office Action, the Examiner took Official Notice (without characterizing it as such), thereby implicitly acknowledging that the cited reference alone fails to anticipate these recitations of claim 1. Specifically, the Examiner stated as follows:

> Alkhatib provides for the encoding/translation of addresses in order to provide more efficient use of storage space, security and compatibility (par 36). <u>This translation may be done via known methods of encryption, compression, or encoding</u> and allows for an entity to secure data at one end while allowing for the receiving entity to extract the information at a later time by unencoding, decoding, decompressing, unencrypting the information using that same information that was used to encode, compress or encrypt the information originally.

(Final Office Action, page 2; Emphasis added.) Paragraph 36 of Alkhatib discloses that "the two domain names can be encoded, compressed, encrypted or otherwise altered to provide more efficient use of storage space, security or compatibility" but fails to disclose or suggest "a key exchanger configured to repeatedly derive a cipher key such that the resulting cipher key changes over time" as recited by claim 1. Thus, the Examiner relied on the above-quoted Official Notice with respect to "a key exchanger configured to repeatedly derive a cipher key such that the resulting cipher key changes over time" as recited by claim 1.

In the response after Final Office action dated December 7, 2010, Appellants timely and specifically requested the Examiner to provide documentary evidence in support for the Official Notice regarding what "methods of encryption, compression, or encoding" are allegedly "known" within the context of the recitations of claim 1. Appellants further requested for such support to include both evidence sufficient to show "a key exchanger configured to repeatedly derive a cipher key such that the resulting cipher key changes over time" as recited in the context of claim 1, as well as a proper rationale for how the supporting evidence would reasonably be combined with Alkhatib. As required by 37 CFR 1.104(d)(2), and as stated by MPEP section 2144.03, "[if] applicant adequately traverses the examiner's assertion of official notice, the examiner <u>must</u> provide documentary evidence in the next Office action if the rejection is to be maintained." (M.P.E.P. § 2144.03.C; Emphasis added.)

However, the Examiner failed to provide any documentary evidence in support of the aforementioned taking of Official Notice. Rather, in the Advisory Action the Examiner instead stated as follows:

> Alkhatib clearly discloses the use of encryption throughout his specification, including but not limited to those portions particularly

> cited in previous office actions. The commonplace usage of such technologies is well known in the art, and insofar as the reference states as much, the Examiner has not felt the need to provide additional secondary references regarding the use of such technologies (see paragraph 14 for example).

(Advisory Action, page 2; Emphasis added.)

Alkhatib mentions that "extraction or identification can be by unencoding, decoding, decompressing, unencrypting," but fails to teach or suggest "a key exchanger configured to repeatedly derive a cipher key such that the resulting cipher key changes over time" as recited by claim 1. Because Alkhatib lacks the requisite disclosure, and further because the Examiner elected not to provide any documentary evidence in support for the taking of Official Notice in the Final Office Action, the rejection of independent claim 1 over Alkhatib must be reversed.

b. *"decrypt, according to a cipher algorithm keyed by the cipher key, the extracted packet header data"*

Alkhatib fails to anticipate to "decrypt" any information "according to a cipher algorithm keyed by the cipher key," let alone to "decrypt, according to a cipher algorithm keyed by the cipher key, the extracted packet header data to determine a restored address" as recited within the context of the claim 1. Alkhatib mentions only in the most general terms that "DNR 148 would need to decode, decompress, unencrypt, etc.," but fails disclose any details at all of these decode, decompress, or unencrypt operations. In particular, Alkhatib fails to disclose or suggest to "decrypt, according to a cipher algorithm keyed by the cipher key, the extracted packet header data" as recited in the context of claim 1.

This lack of disclosure is further evident when considered in the context of the claim. Not only does Alkhatib fail to anticipate to "decrypt, according to a cipher algorithm keyed by the cipher key, the extracted packet header data to determine a restored address," but moreover, Alkhatib further fails to anticipate the recitations within the further context of "to repeatedly derive a cipher key such that the resulting cipher key changes over time" as recited in claim 1 and as discussed above.

As mentioned above, in response to previous arguments the Examiner stated that:

> Alkhatib provides for the encoding/translation of addresses in order to provide more efficient use of storage space, security and compatibility (par 36). This translation may be done via known methods of encryption, compression, or encoding and allows for an entity to secure data at one end while allowing for the receiving entity to extract the information at a later time by unencoding, decoding, decompressing, unencrypting the information using that same information that was used to encode, compress or encrypt the information originally.

(Final Office Action, page 2.) However, as discussed above and in the response after final dated December 7, 2010, Alkhatib fails to disclose "a key exchanger configured to repeatedly derive a cipher key such that the resulting cipher key changes over time" and to "decrypt, according to a cipher algorithm keyed by the cipher key" as recited in the context of claim 1. Rather than disclosing these elements as expressly recited by claim 1, Alkhatib instead includes only the most general disclosure of encryption, such as that "extraction or identification can be by unencoding, decoding, decompressing, unencrypting, etc.," and "if the domain names are compressed, encrypted, encoded, etc., then DNR 148 would need to decode, decompress, unencrypt, etc." (Alkhatib, paragraphs 36 and 67.) Moreover, the cited portions of Alkhatib do not support the assertion that the decoding is done "using that same information that was used to encode, compress or encrypt the information originally" as alleged in the Final Office Action.

Thus, in the response after Final Office action dated December 7, 2010, to the extent that the Examiner took Official Notice that to "decrypt, according to a cipher algorithm keyed by the cipher key, the extracted packet header data to determine a restored address" is allegedly "known" within the context of the recitations of claim 1, Appellants also requested for the Examiner to provide support for such Official Notice in response, as required by MPEP section 2144.03 and 37 CFR 1.104(d)(2), including a rationale how the additional support may reasonably be combined with Alkhatib.

However, rather than providing any documentary evidence, such as a reference or affidavit supporting the Official Notice, the Examiner merely responded by stated that "[the] commonplace usage of such technologies is well known in the art, and insofar as the reference states as much, the

Examiner has not felt the need to provide additional secondary references regarding the use of such technologies." (Advisory Action, page 2.)

Because Alkhatib fails to teach or suggest to "decrypt, according to a cipher algorithm keyed by the cipher key, the extracted packet header data" as recited by claim 1, and further because the Examiner elected not to provide any documentary evidence in support for the taking of Official Notice in the Final Office Action, the rejection of independent claim 1 over Alkhatib must be reversed.

c. *"decrypt, . . . to determine a restored address"*

Independent claim 1 recites in part to "decrypt, according to a cipher algorithm keyed by the cipher key, the extracted packet header data to determine a restored address," within the further context of "a translator configured to restore predetermined portions of packet header information of a data packet." In the Final Office Action, the Examiner cited paragraphs 12, 14, 36, and 67 of Alkhatib as allegedly disclosing the recitations. (Final Office Action, page 5.) Alkhatib discloses that a "domain name" included in data addressed to a DNR may be used by the DNR to determine a "local address." (e.g., Alkhatib, Abstract.) However, the "domain name" and the "local address" of Alkhatib fail to teach or suggest the "restored address" as recited in the context of claim 1.

An exemplary portion of the Specification as originally filed states that:

> The destination ASD peer 35 intercepts the packet … and proceeds to restore the packet header back to its original form. Restoration proceeds similarly to translation: first, packet header data: Identification, Source Host portion of the Source Address (i.e., lower 8-bits), Destination Host portion of the Destination Address (i.e., lower 8-bits), Source Port, Destination Port, Sequence Number, Acknowledgement Number, and Padding are extracted and packed into a byte array. Then the byte array is run through the symmetric cryptographic algorithm to decrypt it, using the negotiated key. The restored parameters are copied into the packet header, overwriting the original fields. The result is a restored header now resembling the original packet header created by the sending host 31. The packet is then forwarded to the receiving host 34, completing delivery.

(Appellants' Specification, paragraph 50; Emphasis added.)

By comparison, Alkhatib discloses to insert a "domain name" into the "Options Field 80" of a header or into a data portion 102 of a TCP segment. (Alkhatib, paragraph 48.) Using this inserted "domain name," Alkhatib further discloses to "[translate] that domain name to a local address and send the data to the destination [i.e., send to the translated local address]." (Alkhatib, Abstract; paragraph 52.) In some instances, "information used to represent the domain name could include an encrypted version of the domain name, an encoded version of the domain name, a compressed version of the domain name, etc." (Alkhatib, paragraph 14.) If so, "then DNR 148 would need to decode, decompress, unencrypt, etc." the information to retrieve the domain name. (Alkhatib, paragraph 67.)

Alkhatib fails to disclose or suggest that the "domain name" being decoded, decompressed, or unencrypted is a "<u>restored</u> address" as recited by claim 1. (Emphasis added.) Rather than being a "restored address," this decoded "domain name" is instead an input used by a receiving DNR to allow the DNR to determine "a local address." (Alkhatib, Abstract, paragraph 52.)

Moreover, the "local address" determined in Alkhatib is also not a "restored address" as recited in the context of claim 1, at least because the "local address" is <u>not</u> a portion of an original packet created by the sender and put back into its original form. Rather than being a "restored address," the "local address" of Alkhatib is simply a "local address" translated from the "domain name" using the DNR.

At least because neither the "domain name" nor the "local address" in Alkhatib are a "restored address" as recited in the context of claim 1, Alkhatib further fails to teach or suggest to "decrypt, according to a cipher algorithm keyed by the cipher key, the extracted packet header data to determine a restored address" as recited by claim 1.

For at least these additional reasons, independent claim 1 and all claims that depend therefrom are patentable over Alkhatib.

d. *"place the restored address back into the packet header information of the data packet"*

Independent claim 1 recites in part to "place the restored address back into the packet header information of the data packet." In the Final Office Action, the Examiner stated that:

> (par 12 "the Domain Name Router receives the data, extracts the destination's domain name from the data, translates that domain name to a local address in its stub network and sends the data to the destination; par 14; par 36 "That extraction or identification can be by unencoding, decoding, decompressing, unencrypting, etc"; par 67.)

(Final Office Action, page 5.) Not only does Alkhatib fail to teach or suggest to "determine a restored address" as discussed above, but Alkhatib further fails to teach or suggest to "place the restored address back into the packet header information of the data packet" as recited in the context of claim 1.

Alkhatib discloses that an additional "domain name" data element may be translated into a "local address." (See, Alkhatib, Abstract.) However, as discussed above, the "local address" of Alkhatib is <u>not</u> a portion of an original packet created by the sender and put back into its original form. (e.g., Appellants' Specification, paragraph 50.) Thus, not only does Alkhatib fail to anticipate to "decrypt . . . the extracted packet header data to determine a restored address" as recited by claim 1, but Alkhatib further fails to anticipate "a restored address" within the context of to "place the restored address back into the packet header information of the data packet" as recited in the context of claim 1.

For at least these reasons, independent claim 1 and all claims that depend therefrom are patentable over Alkhatib.

2. Independent Claim 6, 11 And 16

Each of independent claims 1, 6, 11 and 16 was rejected under Section 102(e) as allegedly being anticipated by Alkhatib. While claims 1, 6, 11 and 16 are each of different scope, at least for reasons similar to those given above with regard to the patentability of independent claim 1, independent claims 6, 11, and 16 are patentable over Alkhatib.

For example, as discussed above with regard to independent claim 1, Alkhatib does not teach or suggest "to repeatedly derive a cipher key such that the resulting cipher key changes over time," to "decrypt, according to a cipher algorithm keyed by the cipher key, the extracted packet header data to determine a restored address," and to "place the restored address back into the packet header information of the data packet" as recited in the context of claim 1. Independent claims 6,

11, and 16 each includes like recitations, although claim 6 recites "decrypting" and "placing," claim 11 recites "means for repeatedly deriving," "means for decrypting," and "means for placing," and claim 16 recites to "repeatedly derive."

Accordingly, for at least similar reasons to those discussed above with regard to independent claim 1, independent claims 6, 11, and 16 and all claims that depend therefrom are patentable over Alkhatib.

3. Claim 25 Is Separately Patentable

Claim 25 depends from independent claim 1. Thus, claim 25 is patentable at least for reasons similar to those discussed above with respect to independent claim 1. Moreover, claim 25 further recites in part "the host portion of the address having been translated without the network portion also being translated, and wherein said translator is configured to restore the host portion of the address without also restoring the network portion of the address."

In the Final Office Action, the Examiner cited paragraph 67 of Alkhatib as allegedly disclosing the recitations of claim 25, without explanation. (Final Office Action, page 6.) However, as argued in subsection (a) below, Alkhatib discloses to overwrite the entire destination address, not "to restore the host portion of the address without also restoring the network portion of the address" as recited by claim 25, let alone within the further context of "the host portion of the address having been translated without the network portion also being translated."

In response to previous arguments, the Examiner cited to portions of Alkhatib that disclose potentially overwriting the entire destination address multiple times using multiple DNRs. Nevertheless, as argued in subsection (b), overwriting the entire destination address multiple times fails to teach or suggest "to restore the host portion of the address without also restoring the network portion of the address" as recited in the context of claim 25.

a. *"the host portion of the address having been translated without the network portion also being translated..."*

Appellants' Specification includes the following exemplary disclosure with respect to "the host portion of the address having been translated without the network portion also being translated":

> [0038] The encrypted portions of the packet header are those portions relating to the source and destination hosts 31, 34 and packet sequencing information. In this embodiment, the packets include class-C addresses routable over the Internet. Class-C addresses use 24 bits for the network portion of the address, and 8 bits for the individual machine portion of the address. Those skilled in the art will appreciate that ASD could be tailored for use with other address classes, in which case the number of bits used for the network address will differ. Note, however, that the network portions of the source and destination addresses (e.g., the upper 24 bits of a class-C packet) are not encrypted, thus allowing the packets to be routed on the Internet 36.

(Appellants' Specification, paragraph 38.) With respect to "wherein said translator is configured to restore the host portion of the address without also restoring the network portion of the address," Appellants' Specification discloses that:

> Restoration proceeds similarly to translation: first, packet header data: Identification, Source Host portion of the Source Address (i.e., lower 8-bits), Destination Host portion of the Destination Address (i.e., lower 8-bits), Source Port, Destination Port, Sequence Number, Acknowledgement Number, and Padding are extracted and packed into a byte array.

(Appellants' Specification, paragraph 48.)

By comparison, Alkhatib discloses to overwrite the <u>entire</u> destination address of a data unit with a "local address." (e.g., Alkhatib, paragraph 68.) Cited paragraph 67 of Alkhatib discloses in part that:

> FIG. 10 describes the steps performed by DNR 138 when it receives the IP packet from host 150. In step 502, DNR 138 receives the IP packet. In step 504, DNR 138 identifies the destination's domain name from the packet. Identifying the domain name could include looking for the domain name in the header, data portion or other location in an IP packet, TCP segment, application data, etc. Identifying the domain name may include reading an ASCII string. Alternatively, if the domain names are compressed, encrypted, encoded, etc., then DNR 148 would need to decode, decompress, unencrypt, etc. In step 506, DNR 138 translates the destination domain name to a local address and in step 508 the packet is routed to the destination with the local address.

(Alkhatib, paragraph 67.) Alkhatib further discloses that "the global address for DNR 138 in the IP packet is replaced with the local address in the table" and "the checksum for the IP header is adjusted if necessary." (Alkhatib, paragraph 68; Emphasis added.) Moreover, as cited earlier in the Final Office Action, paragraph 15 of Alkhatib states that:

> In one embodiment, the data unit sent to the Domain Name Router includes a global IP address for the Domain Name Router. After translating the domain name to a local address, the Domain Name Router will replace the global address for the Domain Name Router with the local address of the destination. The step of replacing the global address with the local address can include adjusting any appropriate checksums or any other necessary fields in the data unit.

(Alkhatib, paragraph 15; Emphasis added.)

Because Alkhatib discloses to overwrite the entire destination address of the data unit with "the local address of the destination," Alkhatib accordingly replaces both the network portion of the destination address and also the host portion of the destination address. Thus, Alkhatib fails to disclose or suggest "the host portion of the address having been translated without the network portion also being translated" as recited by claim 25, let alone "wherein said translator is configured to restore the host portion of the address without also restoring the network portion of the address" as further recited by claim 25. For at least these reasons, claim 25 is separately patentable over Alkhatib.

b. Response to Previous Arguments

In response to previous arguments, the Examiner stated that:

> Alkhatib provides for a variety of embodiments whereby different portions of a packet's address may be translated while others remain untranslated and whereby different portions of the addresses may be placed in different areas of the headers (par 56). For example, in paragraph 67 the situation arises in which the routing and translation serves to transport the packet to a secondary location where yet another translation must be done in order to locate a particular address within a larger address space.

(Final Office Action, page 3.) In the Advisory Action, the Examiner also stated that:

> Applicant's remarks with regards to claim 25 are equally unpersuasive insofar as Alkhatib discloses the translation of addresses from their

> exchanged form back to the actual addresses, and placement of those addresses back into the packet headers in order to transmit the packet along to its final destination (par 67). In view of the reference in its entirety, the Examiner maintains those rejections presented in her outstanding office action.

(Advisory Action, page 2.) Appellants respectfully disagree. Alkhatib discloses that a "domain name" is translated into a "local address," not into "different portions of a packet's address." (See Alkhatib, Abstract, Fig. 10, paragraphs 12, 15, 52 and 67, and claims 1, 21 and 41.) While Alkhatib discloses potentially overwriting the entire destination address multiple times using multiple DNRs, Alkhatib fails to teach or suggest "the host portion of the address having been translated without the network portion also being translated, and wherein said translator is configured to restore the host portion of the address without also restoring the network portion of the address" as recited by claim 25.

Cited paragraph 56 discloses that "FIGS. 7-10 are flow charts which describe the process for sending data according to the present invention." (Alkhatib, paragraph 56.) The paragraph then discusses aspects of the hosts, and states that: "a message is being sent from host 150 to host 132," "host 132 has a local address and host 150 has a global address," "it is assumed that host 150 and 132 are computers," and "host 150 and 152 can be other electronic devices." (Id.) However this disclosure bears no relation to "the host portion of the address having been translated without the network portion also being translated, and wherein said translator is configured to restore the host portion of the address without also restoring the network portion of the address" as recited by claim 25.

Cited paragraph 67 discloses in relevant part that:

> FIG. 11 describes one exemplar embodiment for performing the step of translating the destination domain name to a local address (step 506 of FIG. 10). … Translating a domain name can include less than all of the steps of FIG. 11. In step 512, DNR 138 looks up the domain name in a DNR table stored in its memory or other storage device. The DNR table includes domain names and corresponding local addresses. In one embodiment, the DNR table could also include Ethernet addresses. It is also possible that the local network includes multiple DNRs, forming a tree. Thus, the entry in the DNR table for a particular domain name could be just an address for another DNR.

> The packet would then be sent to another DNR, and the second DNR that would then use the domain name to find the final (or next) local address to the destination or another DNR, etc. The DNR table can be set up manually by the administrator for the network or may be set up automatically through embedded software, firmware or hardware.

(Alkhatib, paragraph 67; Emphasis added.) While Alkhatib discloses that a "packet would then be sent to another DNR, and the second DNR that would then use the domain name to find the final (or next) local address to the destination or another DNR," such disclosure bears no relation to "wherein said translator is configured to restore the host portion of the address without also restoring the network portion of the address" as recited by claim 25. Rather, each forward to a next DNR simply overwrites the entire destination address of the data unit. Overwriting the entire destination address multiple times; however, does not teach or suggest "wherein said translator is configured to restore the host portion of the address without also restoring the network portion of the address" as recited in the context of claim 25.

Accordingly, at least for the reasons discussed above and in previous papers, claim 25 is separately patentable over Alkhatib.

4. Claims 27, 29 And 31 Are Separately Patentable

Claims 27, 29 and 31 were rejected under Section 102(e) as allegedly being anticipated by Alkhatib. (Final Office Action, pages 6-7.) As discussed above with regard to claim 25, Alkhatib does not teach or suggest at least "to restore the host portion of the address without also restoring the network portion of the address." Claims 27, 29, and 31 depend from different base claims. Nevertheless, at least for similar reasons, dependent claims 27, 29 and 31 are also separately patentable over Alkhatib.

For example, claim 27 depends from independent claim 6 and recites in part "wherein restoring predetermined portions of packet header information includes restoring the host portion of the address without also restoring the network portion of the address." Claim 29 depends from independent claim 11 and recites in part "wherein said means for translating predetermined portions of packet header information is configured to restore the host portion of the address without also restore the network portion of the address." Claim 31 depends from independent claim 16 and

recites in part "wherein the bastion host is further configured to restore predetermined portions of packet header information including restoring the host portion of the address without also restoring the network portion of the address."

Thus, while claims 25, 27, 29, and 31 are each of different scope, at least for reasons similar to those given above for the patentability of claim 25, claims 27, 29, and 31 are also separately patentable over Alkhatib.

CONCLUSION

In view of the above analysis, a reversal of the rejections of record is respectfully requested of this Honorable Board.

It is believed that any fees associated with the filing of this paper are identified in an accompanying transmittal. However, if any additional fees are required, they may be charged to Deposit Account No. 18-0013, under Order No. 65632-0534, from which the undersigned is authorized to draw. To the extent necessary, a petition for extension of time under 37 C.F.R. § 1.136 is hereby made, the fee for which should be charged against the aforementioned account.

Dated: March 7, 2011

Respectfully submitted,

Electronic signature: /Isaac T. Slutsky/
Michael B. Stewart
Registration No.: 36,018
Isaac T. Slutsky
Registration No.: 64,620
RADER, FISHMAN & GRAUER PLLC
Correspondence Customer Number: 25537
Attorneys for Appellants

APPENDIX A

Pursuant to 37 CFR § 41.37(c)(viii), the following listing provides a copy of the claims involved in the appeal.

1. An apparatus for detecting adversarial activity on a network, comprising:

a memory configured to store a host table;

a key exchanger configured to repeatedly derive a cipher key such that the resulting cipher key changes over time;

a translator configured to restore predetermined portions of packet header information of a data packet, the packet header information including a network portion of a destination address routable over a wide area network and an encrypted host portion of the address identifying a destination host, the restoration including to:

extract, from the packet header information, predetermined portions of packet header data including the encrypted host portion of the address,

decrypt, according to a cipher algorithm keyed by the cipher key, the extracted packet header data to determine a restored address, and

place the restored address back into the packet header information of the data packet;

a mapping device configured to map the restored address to the host table;

a host resolution device configured to issue a request to the network to resolve the restored address when the restored address does not match an entry in the host table and to supplement the host table with the restored address upon receipt of a reply to the request that indicates that the restored address is valid; and

an actuator configured to trigger a security device when the restored address does not match an entry in the host table.

2. An apparatus as set forth in Claim 1, wherein the security device is a logging device configured to log the data packet.

3. An apparatus as set forth in Claim 1, wherein the security device is configured to signal an alarm when triggered.

4. An apparatus as set forth in Claim 1, wherein said host resolution device is configured to derive the host table using an address resolution protocol.

5. An apparatus as set forth in Claim 1, further comprising:

a network device configured to place the data packet onto a network when the restored address maps to the host table.

6. A method for detecting adversarial activity on a network, comprising:

storing a host table;

repeatedly deriving a cipher key such that the resulting cipher key changes over time;

restoring predetermined portions of packet header information of a data packet, the packet header information including a network portion of a destination address routable over a wide area network and an encrypted host portion of the address identifying a destination host, the restoring including:

extracting, from the packet header information, predetermined portions of packet header data including the encrypted host portion of the address,

decrypting, according to a cipher algorithm keyed by the cipher key, the extracted packet header data to determine a restored address and

placing the restored address back into the packet header information of the data packet;

mapping the restored address to the host table;

issuing a request to the network to resolve the restored address when the restored address does not match an entry in the host table and supplementing the host table with the restored address upon receipt of a reply to the request that indicates that the restored address is valid; and

triggering a security device when the restored address does not match an entry in the host table.

7. A method as set forth in Claim 6, further comprising:

logging the data packet when the address does not match an entry in the host table.

8. A method as set forth in Claim 6, further comprising:

signaling an alarm when the security device is triggered.

9. A method as set forth in Claim 6, further comprising: deriving the host table using an address resolution protocol.

10. A method as set forth in Claim 6, further comprising:

placing the data packet onto a network when the restored address maps to the host table.

11. A device for detecting adversarial activity on a network, comprising:

means for storing a host table;

means for repeatedly deriving a cipher key such that the resulting cipher key changes over time;

means for restoring predetermined portions of packet header information of a data packet, the packet header information including a network portion of a destination address routable over a wide area network and an encrypted host portion of the address identifying a destination host, the means for restoring including:

means for extracting, from the packet header information, predetermined portions of packet header data including the encrypted destination host portion of the address,

means for decrypting, according to a cipher algorithm keyed by the cipher key, the extracted packet header data to determine a restored address and

means for placing the restored address back into the packet header information of the data packet;

means for mapping the restored address to the host table;

means for issuing a request to the network to resolve the restored address when the restored address does not match an entry in the host table and supplementing the host table with the restored address upon receipt of a reply to the request that indicates that the restored address is valid; and

means for triggering a security device when the restored address does not match an entry in the host table.

12. A device as set forth in Claim 11, further comprising:

means for logging the data packet when the restored address does not match an entry in the host table.

13. A device as set forth in Claim 11, further comprising:

means for signaling an alarm when the security device is triggered.

14. A device as set forth in Claim 11, further comprising: means for deriving the host table using an address resolution protocol.

15. A device as set forth in Claim 11, further comprising:

means for placing the data packet onto a network when the restored address maps to the host table.

16. A bastion host comprising at least one computing device adapted for processing packet header information of a data packet, the bastion host being configured to:

store a host table;

repeatedly derive a cipher key such that the resulting cipher key changes over time;

restore predetermined portions of packet header information of a data packet, the packet header information including a network portion of a destination address routable over a wide area network and an encrypted host portion of the address identifying a destination host, the restoring including to:

extract, from the packet header information, predetermined portions of packet header data including the encrypted host portion of the address,

decrypt, according to a cipher algorithm keyed by the cipher key, the extracted packet header data to determine a restored address and

place the restored address back into the packet header information of the data packet;

map the restored address to the host table;

issuing a request to the network to resolve the restored address when the restored address does not match an entry in the host table and supplement the host table with the restored address upon receipt of a reply to the request that indicates that the restored address is valid; and

trigger a security device when the restored address does not match an entry in the host table.

17. The bastion host as set forth in Claim 16, the bastion host being further configured to log the data packet when the restored address does not match an entry in the host table.

18. The bastion host as set forth in Claim 16, the bastion host being further configured to signal an alarm when the security device is triggered.

19. The bastion host as set forth in Claim 16, the bastion host being further configured to derive the host table using an address resolution protocol.

20. The bastion host as set forth in Claim 16, the bastion host being further configured to place the data packet onto a network when the restored address maps to the host table.

25. An apparatus as set forth in Claim 1, the host portion of the address having been translated without the network portion also being translated, and wherein said translator is configured to restore the host portion of the address without also restoring the network portion of the address.

26. An apparatus as set forth in Claim 1, wherein the data packet includes a translated packet header with a plurality of fields carrying packet header information, the translated packet header including the translated packet header information in one or more predetermined fields of the translated packet header interspersed with un-translated packet header information in fields other than the one or more fields of the translated packet header, and

wherein said translator is configured to restore at least a portion of the packet header information in the one or more predetermined fields.

27. A method as set forth in Claim 6, the host portion of the address having been translated without the network portion also being translated, and wherein restoring predetermined portions of packet header information includes restoring the host portion of the address without also restoring the network portion of the address.

28. A method as set forth in Claim 6, wherein the data packet includes a translated packet header with a plurality of fields carrying packet header information, the translated packet header including the translated packet header information in one or more predetermined fields of the translated packet header interspersed with un-translated packet header information in fields other than the one or more fields of the translated packet header, and wherein restoring predetermined portions of packet header information comprises:

restoring at least a portion of the packet header information in the one or more predetermined fields.

29. A device as set forth in Claim 11, the host portion of the address having been translated without the network portion also being translated, and wherein said means for translating predetermined portions of packet header information is configured to restore the host portion of the address without also restore the network portion of the address.

30. A device as set forth in Claim 11, wherein the data packet includes a translated packet header with a plurality of fields carrying packet header information, the translated packet header including the translated packet header information in one or more predetermined fields of the translated packet header interspersed with un-translated packet header information in fields other than the one or more fields of the translated packet header, and wherein said means for restoring predetermined portions of packet header information is configured to restore at least a portion of the packet header information in the one or more predetermined fields.

31. A bastion host as set forth in Claim 16 the host portion of the address having been translated without the network portion also being translated, and wherein the bastion host is further configured to restore predetermined portions of packet header information including restoring the host portion of the address without also restoring the network portion of the address.

32. A bastion host as set forth in Claim 16, wherein the data packet includes a translated packet header with a plurality of fields carrying packet header information, the translated packet header including the translated packet header information in one or more predetermined fields of the translated packet header interspersed with un-translated packet header information in fields other than the one or more fields of the translated packet header, and wherein the bastion host is further configured to restore predetermined portions of packet header information including:

restoring at least a portion of the packet header information in the one or more predetermined fields of the header.

APPENDIX B

Not applicable – in this Appeal, Appellants do not rely on any evidence submitted pursuant to 37 C.F.R. §§ 1.130, 1.131, or 1.132, or on any other evidence entered by the Examiner.

APPENDIX C

Not applicable – no related proceedings are referenced in Section II above; hence, copies of decisions in related proceedings are not provided.